

AFFIDAVIT IN SUPPORT OF
CRIMINAL COMPLAINT

I, Leah Bogdanowicz, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I submit this affidavit in support of finding probable cause to issue a criminal complaint charging PRADIP SAU, DEBALINA SEN, and NASIR HUSSAIN, with conspiracy to commit wire fraud from in or about May 2019 through the present, in violation of 18 U.S.C. § 1349.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI), an agency of the Department of Justice. I am empowered to investigate and make arrests for offenses of Title 18 of the United States Code. I have been a Special Agent of the FBI since December 2021. Prior to my employment with the FBI, I worked at PricewaterhouseCoopers in their Risk Assurance division for almost ten years, ending my employment as a Senior Manager. During my time at PricewaterhouseCoopers, I performed information technology audits and consultations on several Fortune 500 companies, including banking clients and other large financial institutions. My education includes a master's degree in Accounting and a minor in Information Systems.

3. During my employment with the FBI, I have been trained in various aspects of law enforcement, including criminal and national security investigations. I have received training and investigated a variety of federal crimes involving cyber intrusions and computer fraud. I have experience regarding these federal violations through my daily investigative responsibilities and extensive training. For example, I have attended classes and trainings dealing with computer

crimes and fraud, including how computer networks operate, methods employed by criminals to infiltrate computer networks and commit other crimes, the purpose of the intrusions, and the numerous types of fraudulent schemes that perpetrators of computer crimes carry out after gaining access to computer networks.

4. As a Special Agent of the FBI, I am responsible for conducting criminal investigations of criminal statutes contained in Title 18 of the United States Code, including crimes related to computer intrusions. I have participated in the investigation of individuals for violations of Title 18 of the United States Code. Through these investigations, my training, experience, and conversations with other law enforcement officers, I have become familiar with communication methods used by criminal subjects in various types of criminal enterprises, including communication by cellular telephones, Internet-based communication applications, and social media sites.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

6. On May 26, 2022, I received an Internet Crime Complaint Center (IC3) complaint, which described how an unidentified cyber actor or actors (hereinafter “the cyber actor”) sent an email to an elderly Vermont resident (Victim 1), claiming to be a member of the “Geek Squad”, the common name for a computer repair group out of a major chain retailer. The message was regarding a \$329.99 USD annual renewal for an accounting software package.

Victim 1 contacted the telephone number denoted in the email and spoke to the cyber actor to discuss reversing the renewal charge. The cyber actor, pretending to be a member of Geek Squad, instructed Victim 1 to download software to their computer, which allows for remote access and remote control of computer software. Victim 1 allowed the cyber actor to take remote control of the laptop using the downloaded software. The cyber actor instructed Victim 1 to log into their banking system during the remote session.

7. Shortly after control was established by the cyber actor and during the phone call with the cyber actor, Victim 1 noticed a \$25,000 USD deposit into their checking account. Unknown to Victim 1 at the time, the cyber actor had transferred the \$25,000 USD from Victim 1's savings account to Victim 1's checking account. The cyber actor told Victim 1 that the \$25,000 USD checking deposit was intended to be a \$250 USD refund for the \$329.99 USD charge and the additional zeros were accidental. To correct the payment, the cyber actor instructed Victim 1 to make a \$25,000 USD wire for repayment. Victim 1 followed the cyber actor's instructions and paid \$25,000 USD in a single payment to the cyber actor's bank account on May 23, 2022. A few days later, Victim 1 was reviewing their bank statements and saw that the money came from their own savings account and realized that they had been scammed.

8. A second victim (Victim 2), a Tennessee resident, was identified through investigative research, and reported being scammed through a similar scheme. Victim 2 reported that in March 2021, they were contacted by a cyber actor pretending to be an employee of Amazon. The aforementioned fact pattern of remote access, savings to checking transfer, and money wiring was followed. Victim 2 was able to provide law enforcement the routing and account number of the account into which the proceeds were transferred. Based on that

information, and process issued to the bank, I learned that the account holder for the account receiving the scammed funds was Pradip Sau¹, hereinafter “Sau.”

9. A third victim (Victim 3), a South Carolina resident, was identified through investigative research, and reported being scammed through a similar scheme. Victim 3 reported that in January 2022, they were contacted by a cyber actor who claimed that Victim 3 had a problem with their computer. The aforementioned fact pattern of remote access, savings to checking transfer, and money wiring was followed. Victim 3 was able to provide law enforcement the routing and account number of the account into which the proceeds were transferred. Based on that information, and process issued to the bank, I learned that the account holder for the account receiving the scammed funds was Debalina Sen², hereinafter “Sen”, who is the wife³ of Sau.

¹ According to documents provided by Customs and Border Protection, Sau entered the United States (US) in December 2018 on a J-1 visa, which is a visa provided to international individuals who come the US on a cultural exchange program. Sau’s visa application states that his exchange program is through the Guru Nanak Institute of Hotel Management, which is a hotel management school in India. According to Accurint data, all of Sau’s permanent home addresses since 2019 have been in Florida. On a J-1 visa, individuals are granted a US Social Security number, which is one of the required forms of identification to open a bank account at financial institutions in the US.

² According to documents provided by Customs and Border Protection, Sen entered the United States (US) in May 2018 on a J-1 visa, which is a visa provided to international individuals who come the US on a cultural exchange program. Sen’s visa application states that her exchange program is through the Guru Nanak Institute of Hotel Management, which is a hotel management school in India. According to Accurint data, all of Sen’s permanent home addresses since 2019 have been in Florida. On a J-1 visa, individuals are granted a US Social Security number, which is one of the required forms of identification to open a bank account at financial institutions in the US.

³ According to a Sumter County Sherriff’s Office police report that was filed in October 2022, Sau and Sen consider each other husband and wife. They were living at 13813 NE 136th Loop, Apartment 1115 Lady Lake, Florida at the time of the police report.

10. Through additional investigative research, I have identified over 200 victims who collectively suffered almost \$3 million USD in attempted losses, and almost \$2.4 million USD in actual losses from scams similar to the scheme described in paragraphs 6 through 9. Victims were connected to each other as they either called the same telephone numbers or sent money to the same bank accounts during the related scams. The vast majority of these victims are considered elderly, as they are over 60 years of age.

11. Based on my investigation, including a review of the routing numbers, account numbers, and corresponding bank records belonging to bank accounts controlled by Sau and Sen, I have identified over 150 of the aforementioned victims who have sent funds through Sau and Sen's bank accounts. Since May 2019, the 150+ victims have suffered collective losses that total approximately \$650,000 USD. According to records provided by Santander Bank, M&T Bank, Truist/SunTrust, Wells Fargo, and TD Bank, Sau and Sen's incomes since May 2019 have not come from paycheck deposits, but instead have consisted of large wire payments (averaging ~\$14,000 USD) and/or moderately sized Zelle payments (averaging ~\$1,400 USD). Each of the names associated with the wire and Zelle payments correspond with the names of the aforementioned 150+ victims. Within a week after each of the deposits, payments via money transfer companies to India would occur, averaging approximately \$1,200 USD each. By breaking down the funds into smaller amounts, I believe that the money is being structured to avoid required reporting regulations for transactions in the US.

12. According to records provided by money transfer companies Western Union, Wise, Remitly, and World Remit, payments from Sau and Sen's accounts were sent to recipients in India. Many payments were associated with Sau and Sen themselves, but several payments

were associated with other individuals using Sau's debit cards or bank accounts. Sen's transactions to India are always sent via cash. Through investigative research, I identified that the other individuals are either current or former students who originally came to the US on a J-1 visa from India. Many of the students have similar backgrounds to Sau and Sen in that their original sponsor for their J-1 visa is in the hospitality industry. Each of the Indian students are associated with an Orlando, Florida address at either Oak Creek Street or Conroy Road.

13. Upon further review of the bank records, Sau's mailing address is 4501 Oak Creek Street Apartment 215 in Orlando, Florida and Sen's mail address is 3735 Conroy Road, Apartment 2230 in Orlando, Florida⁴. As previously mentioned, each of the other Indian students have a similar address on Oak Creek Street or Conroy Road in Orlando, Florida. I believe these students are not actually living at these addresses and the address is just a front for their bank account addresses. Based on the facts that Sau and Sen's bank accounts are receiving victim funds and their and other accounts belonging to Indian students are using Sau's banking information to remit money internationally shortly after the victim funds arrive at his bank, I believe that Sau, Sen, and the several other Indian students are part of a money mule⁵ network in

⁴ Please note, these addresses do not align with the Sumter County Sherriff's Office police report that was filed in October 2022, which stated that Sau and Sen were living at 13813 NE 136th Loop, Apartment 1115 Lady Lake, Florida at the time of the police report.

⁵ The Consumer Financial Protection Bureau defines a money mule as "someone who receives and moves money that came from victims of fraud. Some money mules know they are assisting with criminal activity, but others are unaware that their actions are helping fraudsters." In Sau and Sen's cases, I believe they are knowing money mules as they have engaged in this activity for almost four years (since June 2019) and their bank accounts often show personal purchases with the money used from the victim funds quickly after the funding is deposited into their accounts.

the United States, receiving money through technical scam calls that are supported via computer intrusion and then laundering those victim funds to India.

14. In January 2023, the FBI interviewed suspected money mule Yogesh Yadav, hereinafter “Yadav”, in connection with the same scheme. Yadav moved to Marco Island, Florida in September 2019 from India on a J-1 visa for the hospitality industry. During the course of the interview, Yadav indicated that he had met Sau in Marco Island after a few weeks of living in Florida. After two months of friendship, Yadav was told by Sau that Sau had a side job working for Nasir Hussain, hereinafter “Hussain”, another Indian national in the US who originally came to the US on a J-1 visa for the hospitality industry. Hussain lived in Orlando, Florida. Yadav met with Hussain about a month later and learned that “the work” was to open bank accounts under Yadav’s name at Hussain’s direction. Yadav would receive instruction from Hussain about the email addresses, bank accounts, and phones numbers to use to open the bank accounts. Yadav never received the debit cards or spent money from these bank accounts, and believed Hussain received the debit cards. Yadav received approximately \$10,000 through \$15,000 in Zelle payments from Hussain for “the work” that he performed. Based on this

interview, I believe that Yadav is a money mule who was recruited⁶ by Sau and handled⁷ by Hussain.

15. During the course of the interview of Yadav, banking transactions from US Bank and TD Bank accounts opened by Yadav were shown to Yadav. Several transactions were made on consecutive days by multiple people through different money remittance corporations. Each of the transactions were sent to recipients in India. Refer to the following details for examples:

Money Remitter	Sender Account	Date	Bank	Bank Account Holder	Recipient Account
Pangea	Yogesh Yadav	9/16/21	TD Bank	Yogesh Yadav	Arshad Ali
Western Union	Yogesh Yadav	9/16/21	TD Bank	Yogesh Yadav	Manju Begum
WorldRemit	Nasir Hussain	9/16/21	TD Bank	Yogesh Yadav	Shabana Begum
Wise	Pradip Sau	10/6/21	TD Bank	Yogesh Yadav	Md Moquimuddin
WorldRemit	Yogesh Yadav	10/6/21	TD Bank	Yogesh Yadav	Md Bhawayes
Pangea	Yogesh Yadav	4/16/22	US Bank	Yogesh Yadav	Md Awayes
Wise	Pradip Sau	4/16/22	US Bank	Yogesh Yadav	Md Moquimuddin

During the interview, Yadav denied having made these transactions, as his only money remittance usage is via Remitly and MoneyGram. Yadav also denied knowing any of the names in the “Recipient Account” column.

⁶ According to skopenow.com, “Money mule operations can be established at a small scale, with criminals recruiting mules themselves. Large scale money mule operations usually involve money mule recruiters, sometimes also referred to as “mule herders” and “pickers”. Mule recruiters work on behalf of criminal groups to recruit money mules to move illicit funds through their bank accounts.”

⁷ According to fico.com, “Money muling is often perpetrated by fraud networks, with a money mule ‘handler’ directing the activity of a group of mules.” “Banking behaviors typically associated with an individual mule — including higher-than-normal volumes of deposits and transfers — can trigger fraud alerts in a financial institution.” “For example, a mule handler may sign into multiple mules’ accounts from a single device, which can be a suspicious activity.”

16. During a review of returns from WorldRemit for the transactions above, the associated IP addresses are 2603:9001:2309:e967:ad4e:136a:8fde:b8b9 and 2603:9001:2309:e967:d9ed:5d81:1fb1:a8cd. Both of these IP addresses resolve to Spectrum, also known as Charter Communications, in Orlando, Florida. These IP addresses are aligned with transactions made by Hussain and Yadav (as noted above), but also with transactions made by Pradip Sau and other suspected J-1 Indian money mules. As mentioned in paragraph 14, Hussain lives in Orlando, Florida and received debit cards from Yadav after Yadav opened bank accounts.

17. While reviewing WhatsApp messages between Yadav and Hussain, I read messages on July 4, 2021 discussing travel plans to meet in Chicago. On July 6, 2021, messages between Yadav and Hussain discuss Yadav opening bank accounts at US Bank and Huntington Bank. Messages from Hussain instruct Yadav to open bank accounts with the email “yogeyada123@gmail.com” and “yadoyogi@gmail.com”⁸. In the messages, Yadav responds to Hussain, describing if he is receiving the debit cards or if they are being sent in the mail. Yadav also shares the debit card pin numbers with Hussain. Based on Yadav providing the debit cards to Hussain and the same cards being used by several individuals on the same or consecutive days

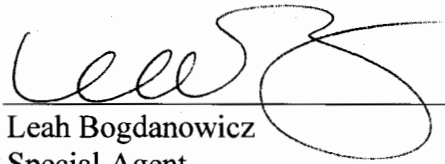
⁸ According to Yadav during the interview described in paragraphs 14 and 15, Yadav’s only e-mail address is “yogi040296@gmail.com”; Yogesh denies having opened the accounts “yogeyada123@gmail.com” and “yadoyogi@gmail.com.” According to returns from Google, the account “yogi040296@gmail.com” contains emails between Yogesh and friends, family, and co-workers, with one other account linked by cookies, whom Yogesh identified as his cousin. The accounts “yogeyada123@gmail.com” and “yadoyogi@gmail.com” contain emails only from banking institutions and the account is linked by cookies to several other suspected J-1 Indian money mules.

from IP addresses in Orlando, Florida, I believe that Hussain is using money mule debit cards that receive victim funds to launder money internationally to India.

CONCLUSION

18. Based on the foregoing, I submit there is probable cause to issue a criminal complaint charging PRADIP SAU, DEBALINA SEN, and NASIR HUSSAIN with conspiracy to commit wire fraud from in or about May 2019 through the present, in violation of 18 U.S.C § 1349.

Dated at Burlington, in the District of Vermont, this 9 th day of May 2023.



Leah Bogdanowicz
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 9th day of May 2023.



HONORABLE KEVIN J. DOYLE
United States Magistrate Judge